Driver NAS ONTAP

Trident

NetApp
January 15, 2026

Sommario

Driver NAS ONTAP

Panoramica del driver NAS ONTAP

Scopri come configurare un backend ONTAP con i driver ONTAP e Cloud Volumes ONTAP NAS.

Dettagli del driver ONTAP NAS

Trident fornisce i seguenti driver di archiviazione NAS per comunicare con il cluster ONTAP . Le modalità di accesso supportate sono: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Autista	Protocollo	Modalità volume	Modalità di accesso supportate	Sistemi di file supportati
`ontap-nas`	NFS SMB	File system	RWO, ROX, RWX, RWOP	"", `nfs` , `smb`
`ontap-nas-economy`	NFS SMB	File system	RWO, ROX, RWX, RWOP	"", `nfs` , `smb`
`ontap-nas-flexgroup`	NFS SMB	File system	RWO, ROX, RWX, RWOP	"", `nfs` , `smb`

- Utilizzo `ontap-san-economy` solo se si prevede che il conteggio dell'utilizzo del volume persistente sia superiore a"limiti di volume ONTAP supportati" .
- Utilizzo `ontap-nas-economy` solo se si prevede che il conteggio dell'utilizzo del volume persistente sia superiore a"limiti di volume ONTAP supportati" e il `ontap-san-economy` il driver non può essere utilizzato.
- Non usare usare `ontap-nas-economy` se prevedi la necessità di protezione dei dati, ripristino di emergenza o mobilità.
- NetApp non consiglia di utilizzare Flexvol autogrow in tutti i driver ONTAP , ad eccezione di ontap-san. Come soluzione alternativa, Trident supporta l'uso della riserva snapshot e ridimensiona di conseguenza i volumi Flexvol.

Permessi utente

Trident prevede di essere eseguito come amministratore ONTAP o SVM, in genere utilizzando `admin` utente del cluster o un `vsadmin` Utente SVM o un utente con un nome diverso che ha lo stesso ruolo.

Per le distribuzioni Amazon FSx for NetApp ONTAP , Trident prevede di essere eseguito come amministratore ONTAP o SVM, utilizzando il cluster `fsxadmin` utente o un `vsadmin` Utente SVM o un utente con un nome diverso che ha lo stesso ruolo. IL `fsxadmin` L'utente è un sostituto limitato dell'utente amministratore del cluster.

Se usi il `limitAggregateUsage` parametro, sono richieste le autorizzazioni di amministratore del cluster. Quando si utilizza Amazon FSx for NetApp ONTAP con Trident, il `limitAggregateUsage` il parametro non funzionerà con il `vsadmin` E `fsxadmin` account utente. Se si specifica questo parametro, l'operazione di configurazione non riuscirà.

Sebbene sia possibile creare un ruolo più restrittivo all'interno di ONTAP utilizzabile da un conducente Trident , non lo consigliamo. La maggior parte delle nuove versioni di Trident richiameranno API aggiuntive di cui bisognerebbe tenere conto, rendendo gli aggiornamenti difficili e soggetti a errori.

Prepararsi a configurare un backend con i driver ONTAP NAS

Comprendere i requisiti, le opzioni di autenticazione e le policy di esportazione per la configurazione di un backend ONTAP con driver ONTAP NAS.

Requisiti

- Per tutti i backend ONTAP , Trident richiede che almeno un aggregato sia assegnato all'SVM.
- È possibile eseguire più di un driver e creare classi di archiviazione che puntano all'uno o all'altro. Ad esempio, è possibile configurare una classe Gold che utilizza `ontap-nas` driver e una classe Bronze che utilizza il `ontap-nas-economy` uno.
- Tutti i nodi worker di Kubernetes devono avere installati gli strumenti NFS appropriati. Fare riferimento a"Qui" per maggiori dettagli.
- Trident supporta volumi SMB montati su pod in esecuzione solo su nodi Windows. Fare riferimento a Prepararsi al provisioning dei volumi SMB per i dettagli.

Autenticare il backend ONTAP

Trident offre due modalità di autenticazione di un backend ONTAP .

- Basato su credenziali: questa modalità richiede autorizzazioni sufficienti per il backend ONTAP . Si consiglia di utilizzare un account associato a un ruolo di accesso di sicurezza predefinito, ad esempio `admin` O `vsadmin` per garantire la massima compatibilità con le versioni ONTAP .
- Basato su certificato: questa modalità richiede un certificato installato sul backend affinché Trident possa comunicare con un cluster ONTAP . Qui, la definizione del backend deve contenere valori codificati in Base64 del certificato client, della chiave e del certificato CA attendibile, se utilizzato (consigliato).

È possibile aggiornare i backend esistenti per passare da metodi basati su credenziali a metodi basati su certificati. Tuttavia, è supportato solo un metodo di autenticazione alla volta. Per passare a un metodo di autenticazione diverso, è necessario rimuovere il metodo esistente dalla configurazione del backend.

> Se si tenta di fornire **sia credenziali che certificati**, la creazione del backend fallirà e verrà visualizzato un errore che indica che nel file di configurazione è stato fornito più di un metodo di autenticazione.

Abilita l'autenticazione basata sulle credenziali

Trident richiede le credenziali di un amministratore con ambito SVM/cluster per comunicare con il backend ONTAP . Si consiglia di utilizzare ruoli standard predefiniti come `admin` O `vsadmin` . Ciò garantisce la compatibilità futura con le future versioni ONTAP che potrebbero esporre API di funzionalità da utilizzare nelle future versioni Trident . È possibile creare e utilizzare un ruolo di accesso di sicurezza personalizzato con Trident, ma non è consigliato.

Un esempio di definizione del backend sarà simile a questo:

YAML

```yaml
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
credentials:
  name: secret-backend-creds
```

JSON

```json
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "credentials": {
        "name": "secret-backend-creds"
    }
}
```

Tieni presente che la definizione del backend è l'unico posto in cui le credenziali vengono archiviate in testo normale. Dopo aver creato il backend, i nomi utente e le password vengono codificati con Base64 e memorizzati come segreti Kubernetes. La creazione/aggiornamento di un backend è l'unico passaggio che richiede la conoscenza delle credenziali. Si tratta pertanto di un'operazione riservata esclusivamente all'amministratore, che deve essere eseguita dall'amministratore di Kubernetes/archiviazione.

Abilita l'autenticazione basata su certificato

I backend nuovi ed esistenti possono utilizzare un certificato e comunicare con il backend ONTAP . Nella definizione del backend sono richiesti tre parametri.

- clientCertificate: valore codificato in Base64 del certificato client.
- clientPrivateKey: valore codificato in Base64 della chiave privata associata.
- trustedCACertificate: valore codificato in Base64 del certificato CA attendibile. Se si utilizza una CA attendibile, è necessario fornire questo parametro. Questo può essere ignorato se non viene utilizzata alcuna CA attendibile.

Un flusso di lavoro tipico prevede i seguenti passaggi.

Passi

1. Genera un certificato client e una chiave. Durante la generazione, impostare il nome comune (CN) sull'utente ONTAP con cui effettuare l'autenticazione.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=vsadmin"
```

2. Aggiungere un certificato CA attendibile al cluster ONTAP . Questa operazione potrebbe essere già gestita dall'amministratore dell'archiviazione. Ignora se non viene utilizzata alcuna CA attendibile.

```
security certificate install -type server -cert-name <trusted-ca-cert-
name> -vserver <vserver-name>
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled
true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca
<cert-authority>
```

3. Installare il certificato client e la chiave (dal passaggio 1) sul cluster ONTAP .

```
security certificate install -type client-ca -cert-name <certificate-
name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```

4. Conferma che il ruolo di accesso alla sicurezza ONTAP supporta `cert` metodo di autenticazione.

```
security login create -user-or-group-name vsadmin -application ontapi
-authentication-method cert -vserver <vserver-name>
security login create -user-or-group-name vsadmin -application http
-authentication-method cert -vserver <vserver-name>
```

5. Verifica l'autenticazione utilizzando il certificato generato. Sostituire < ONTAP Management LIF> e <nome vserver> con l'IP Management LIF e il nome SVM. È necessario assicurarsi che la politica di servizio del LIF sia impostata su `default-data-management` .

```
curl -X POST -Lk https://<ONTAP-Management-
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp
xmlns="http://www.netapp.com/filer/admin" version="1.21"
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. Codifica il certificato, la chiave e il certificato CA attendibile con Base64.

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. Creare il backend utilizzando i valori ottenuti dal passaggio precedente.

```
cat cert-backend-updated.json
{
"version": 1,
"storageDriverName": "ontap-nas",
"backendName": "NasBackend",
"managementLIF": "1.2.3.4",
"dataLIF": "1.2.3.8",
"svm": "vserver_test",
"clientCertificate": "Faaaakkkkeeee...Vaaalllluuuueeee",
"clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
"storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+------------+----------------+--------------------------------------
+--------+---------+
|    NAME    | STORAGE DRIVER |                 UUID                 |
STATE  | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |       9 |
+------------+----------------+--------------------------------------
+--------+---------+
```

Aggiorna i metodi di autenticazione o ruota le credenziali

È possibile aggiornare un backend esistente per utilizzare un metodo di autenticazione diverso o per ruotare le credenziali. Funziona in entrambi i modi: i backend che utilizzano nome utente/password possono essere aggiornati per utilizzare certificati; i backend che utilizzano certificati possono essere aggiornati per utilizzare nome utente/password. Per fare ciò, è necessario rimuovere il metodo di autenticazione esistente e aggiungere il nuovo metodo di autenticazione. Quindi utilizzare il file backend.json aggiornato contenente i parametri richiesti per eseguire `tridentctl update backend`.

```
cat cert-backend-updated.json
```

```
{
"version": 1,
"storageDriverName": "ontap-nas",
"backendName": "NasBackend",
"managementLIF": "1.2.3.4",
"dataLIF": "1.2.3.8",
"svm": "vserver_test",
"username": "vsadmin",
"password": "password",
"storagePrefix": "myPrefix_"
}
```

```
#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+------------+----------------+--------------------------------------
+--------+---------+
|    NAME    | STORAGE DRIVER |                 UUID                 |
STATE   | VOLUMES |
+------------+----------------+--------------------------------------
+--------+---------+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |       9 |
+------------+----------------+--------------------------------------
+--------+---------+
```

Quando si ruotano le password, l'amministratore dell'archiviazione deve prima aggiornare la password per l'utente su ONTAP. Segue un aggiornamento del backend. Durante la rotazione dei certificati, è possibile aggiungere più certificati all'utente. Il backend viene quindi aggiornato per utilizzare il nuovo certificato, dopodiché il vecchio certificato può essere eliminato dal cluster ONTAP .

L'aggiornamento di un backend non interrompe l'accesso ai volumi già creati, né influisce sulle connessioni ai volumi effettuate in seguito. Un aggiornamento del backend riuscito indica che Trident può comunicare con il backend ONTAP e gestire le future operazioni sui volumi.

Crea un ruolo ONTAP personalizzato per Trident

È possibile creare un ruolo cluster ONTAP con privilegi minimi in modo da non dover utilizzare il ruolo di amministratore ONTAP per eseguire operazioni in Trident. Quando si include il nome utente in una configurazione backend Trident , Trident utilizza il ruolo del cluster ONTAP creato per eseguire le operazioni.

Fare riferimento a"Generatore di ruoli personalizzati Trident" per ulteriori informazioni sulla creazione di ruoli personalizzati Trident .

Utilizzo di ONTAP CLI

1. Crea un nuovo ruolo utilizzando il seguente comando:

```
security login role create <role_name\> -cmddirname "command" -access all
–vserver <svm_name\>
```

2. Crea un nome utente per l'utente Trident :

```
security login create -username <user_name\> -application ontapi
-authmethod <password\> -role <name_of_role_in_step_1\> –vserver
<svm_name\> -comment "user_description"
```

3. Assegna il ruolo all'utente:

```
security login modify username <user_name\> –vserver <svm_name\> -role
<role_name\> -application ontapi -application console -authmethod
<password\>
```

Utilizzo di System Manager

Eseguire i seguenti passaggi in ONTAP System Manager:

1. **Crea un ruolo personalizzato**:
   a. Per creare un ruolo personalizzato a livello di cluster, selezionare **Cluster > Impostazioni**.

      (Oppure) Per creare un ruolo personalizzato a livello SVM, selezionare **Archiviazione > VM di archiviazione > `required SVM` > Impostazioni > Utenti e ruoli**.

   b. Selezionare l'icona della freccia (→) accanto a **Utenti e ruoli**.
   c. Selezionare **+Aggiungi** in **Ruoli**.
   d. Definisci le regole per il ruolo e clicca su **Salva**.
2. **Assegnare il ruolo all'utente Trident *: + Eseguire i seguenti passaggi nella pagina *Utenti e ruoli**:
   a. Selezionare Aggiungi icona **+** in **Utenti**.
   b. Selezionare il nome utente richiesto e selezionare un ruolo nel menu a discesa per **Ruolo**.
   c. Fare clic su **Salva**.

Per maggiori informazioni consultare le seguenti pagine:

- "Ruoli personalizzati per l'amministrazione di ONTAP"O"Definisci ruoli personalizzati"
- "Lavorare con ruoli e utenti"

Gestire le policy di esportazione NFS

Trident utilizza criteri di esportazione NFS per controllare l'accesso ai volumi di cui si occupa.

Trident offre due opzioni quando si lavora con le politiche di esportazione:

- Trident può gestire dinamicamente la politica di esportazione autonomamente; in questa modalità di funzionamento, l'amministratore dell'archiviazione specifica un elenco di blocchi CIDR che rappresentano indirizzi IP ammissibili. Trident aggiunge automaticamente alla policy di esportazione gli IP dei nodi applicabili che rientrano in questi intervalli al momento della pubblicazione. In alternativa, se non vengono specificati CIDR, tutti gli IP unicast con ambito globale trovati sul nodo su cui viene pubblicato il volume verranno aggiunti alla policy di esportazione.
- Gli amministratori di storage possono creare una policy di esportazione e aggiungere regole manualmente. Trident utilizza la policy di esportazione predefinita, a meno che non venga specificato un nome diverso nella configurazione.

Gestire dinamicamente le politiche di esportazione

Trident offre la possibilità di gestire dinamicamente le policy di esportazione per i backend ONTAP . Ciò consente all'amministratore dell'archiviazione di specificare uno spazio di indirizzamento consentito per gli IP dei nodi worker, anziché definire manualmente regole esplicite. Semplifica notevolmente la gestione delle policy di esportazione: le modifiche alle policy di esportazione non richiedono più un intervento manuale sul cluster di storage. Inoltre, ciò consente di limitare l'accesso al cluster di archiviazione solo ai nodi worker che montano volumi e hanno IP compresi nell'intervallo specificato, supportando una gestione automatizzata e dettagliata.

> Non utilizzare Network Address Translation (NAT) quando si utilizzano criteri di esportazione dinamici. Con NAT, il controller di archiviazione vede l'indirizzo NAT frontend e non l'indirizzo host IP effettivo, quindi l'accesso verrà negato se non viene trovata alcuna corrispondenza nelle regole di esportazione.

Esempio

Ci sono due opzioni di configurazione che devono essere utilizzate. Ecco un esempio di definizione del backend:

```
---
version: 1
storageDriverName: ontap-nas-economy
backendName: ontap_nas_auto_export
managementLIF: 192.168.0.135
svm: svm1
username: vsadmin
password: password
autoExportCIDRs:
  - 192.168.0.0/24
autoExportPolicy: true
```

> Quando si utilizza questa funzionalità, è necessario assicurarsi che la giunzione radice nella SVM disponga di una policy di esportazione creata in precedenza con una regola di esportazione che consenta il blocco CIDR del nodo (ad esempio la policy di esportazione predefinita). Seguire sempre le best practice consigliate NetApp per dedicare una SVM a Trident.

Ecco una spiegazione del funzionamento di questa funzionalità utilizzando l'esempio sopra riportato:

- `autoExportPolicy`è impostato su `true`. Ciò indica che Trident crea una policy di esportazione per ogni volume fornito con questo backend per il `svm1` SVM e gestire l'aggiunta e l'eliminazione delle regole utilizzando `autoexportCIDRs` blocchi di indirizzi. Finché un volume non viene collegato a un nodo, il volume utilizza una policy di esportazione vuota, senza regole, per impedire l'accesso indesiderato a tale volume. Quando un volume viene pubblicato su un nodo, Trident crea una policy di esportazione con lo stesso nome del qtree sottostante contenente l'IP del nodo all'interno del blocco CIDR specificato. Questi IP verranno aggiunti anche alla policy di esportazione utilizzata dal FlexVol volume padre
  - Per esempio:
    - UUID backend 403b5326-8482-40db-96d0-d83fb3f4daec
    - `autoExportPolicy`impostato su `true`
    - prefisso di archiviazione `trident`
    - Codice UUID PVC a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - qtree denominato trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c crea una politica di esportazione per FlexVol denominata `trident-403b5326-8482-40db96d0-d83fb3f4daec`, una politica di esportazione per il qtree denominato `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` e una politica di esportazione vuota denominata `trident_empty` sull'SVM. Le regole per la policy di esportazione FlexVol saranno un superset di tutte le regole contenute nelle policy di esportazione qtree. La policy di esportazione vuota verrà riutilizzata da tutti i volumi non collegati.
- `autoExportCIDRs`contiene un elenco di blocchi di indirizzi. Questo campo è facoltativo e il suo valore predefinito è ["0.0.0.0/0", "::/0"]. Se non definito, Trident aggiunge tutti gli indirizzi unicast con ambito globale trovati sui nodi worker con pubblicazioni.

In questo esempio, il `192.168.0.0/24` è fornito lo spazio di indirizzamento. Ciò indica che gli IP dei nodi Kubernetes che rientrano in questo intervallo di indirizzi con pubblicazioni verranno aggiunti alla policy di esportazione creata Trident . Quando Trident registra un nodo su cui è in esecuzione, recupera gli indirizzi IP del nodo e li confronta con i blocchi di indirizzi forniti in `autoExportCIDRs` Al momento della pubblicazione, dopo aver filtrato gli IP, Trident crea le regole della policy di esportazione per gli IP client del nodo su cui sta pubblicando.

Puoi aggiornare `autoExportPolicy` E `autoExportCIDRs` per i backend dopo averli creati. È possibile aggiungere nuovi CIDR per un backend gestito automaticamente oppure eliminare i CIDR esistenti. Prestare attenzione quando si eliminano i CIDR per assicurarsi che le connessioni esistenti non vengano interrotte. Puoi anche scegliere di disabilitare `autoExportPolicy` per un backend e ripiegare su una policy di esportazione creata manualmente. Ciò richiederà l'impostazione del `exportPolicy` parametro nella configurazione del backend.

Dopo che Trident crea o aggiorna un backend, puoi controllare il backend utilizzando `tridentctl` o il corrispondente `tridentbackend` CRD:

```
./tridentctl get backends ontap_nas_auto_export -n trident -o yaml
items:
- backendUUID: 403b5326-8482-40db-96d0-d83fb3f4daec
  config:
    aggregate: ""
    autoExportCIDRs:
    - 192.168.0.0/24
    autoExportPolicy: true
    backendName: ontap_nas_auto_export
    chapInitiatorSecret: ""
    chapTargetInitiatorSecret: ""
    chapTargetUsername: ""
    chapUsername: ""
    dataLIF: 192.168.0.135
    debug: false
    debugTraceFlags: null
    defaults:
      encryption: "false"
      exportPolicy: <automatic>
      fileSystemType: ext4
```

Quando un nodo viene rimosso, Trident controlla tutte le policy di esportazione per rimuovere le regole di accesso corrispondenti al nodo. Rimuovendo questo IP del nodo dalle policy di esportazione dei backend gestiti, Trident impedisce i mount non autorizzati, a meno che questo IP non venga riutilizzato da un nuovo nodo nel cluster.

Per i backend già esistenti, aggiornare il backend con `tridentctl update backend` garantisce che Trident gestisca automaticamente le politiche di esportazione. In questo modo vengono create due nuove policy di esportazione denominate in base all'UUID del backend e al nome qtree quando necessario. I volumi presenti nel backend utilizzeranno i criteri di esportazione appena creati dopo essere stati smontati e montati nuovamente.

L'eliminazione di un backend con criteri di esportazione gestiti automaticamente eliminerà il criterio di esportazione creato dinamicamente. Se il backend viene ricreato, viene trattato come un nuovo backend e comporterà la creazione di una nuova policy di esportazione.

Se l'indirizzo IP di un nodo attivo viene aggiornato, è necessario riavviare il pod Trident sul nodo. Trident aggiornerà quindi la politica di esportazione per i backend che gestisce per riflettere questa modifica dell'IP.

Prepararsi al provisioning dei volumi SMB

Con un po' di preparazione aggiuntiva, è possibile eseguire il provisioning dei volumi SMB utilizzando `ontap-nas` conducenti.

È necessario configurare entrambi i protocolli NFS e SMB/CIFS sull'SVM per creare un `ontap-nas-economy` Volume SMB per cluster ONTAP on-premise. La mancata configurazione di uno di questi protocolli causerà il fallimento della creazione del volume SMB.

`autoExportPolicy`non è supportato per i volumi SMB.

Prima di iniziare

Prima di poter effettuare il provisioning dei volumi SMB, è necessario disporre di quanto segue.

- Un cluster Kubernetes con un nodo controller Linux e almeno un nodo worker Windows che esegue Windows Server 2022. Trident supporta volumi SMB montati su pod in esecuzione solo su nodi Windows.
- Almeno un segreto Trident contenente le credenziali di Active Directory. Per generare segreto `smbcreds` :

```
kubectl create secret generic smbcreds --from-literal username=user
--from-literal password='password'
```

- Un proxy CSI configurato come servizio Windows. Per configurare un `csi-proxy` , fare riferimento a"GitHub: Proxy CSI" O"GitHub: Proxy CSI per Windows" per i nodi Kubernetes in esecuzione su Windows.

Passi

1. Per ONTAP on-premise, puoi facoltativamente creare una condivisione SMB oppure Trident può crearne una per te.

   Le condivisioni SMB sono necessarie per Amazon FSx per ONTAP.

   È possibile creare le condivisioni amministrative SMB in uno dei due modi seguenti: utilizzando"Console di gestione Microsoft" Snap-in Cartelle condivise o tramite ONTAP CLI. Per creare le condivisioni SMB utilizzando ONTAP CLI:

   a. Se necessario, creare la struttura del percorso della directory per la condivisione.

      IL `vserver cifs share create` Il comando controlla il percorso specificato nell'opzione -path durante la creazione della condivisione. Se il percorso specificato non esiste, il comando fallisce.

   b. Crea una condivisione SMB associata all'SVM specificato:

```
vserver cifs share create -vserver vserver_name -share-name
share_name -path path [-share-properties share_properties,...]
[other_attributes] [-comment text]
```

   c. Verificare che la condivisione sia stata creata:

```
vserver cifs share show -share-name share_name
```

      Fare riferimento a"Crea una condivisione SMB" per maggiori dettagli.

2. Durante la creazione del backend, è necessario configurare quanto segue per specificare i volumi SMB. Per tutte le opzioni di configurazione del backend FSx for ONTAP , fare riferimento a"Opzioni di configurazione ed esempi di FSx per ONTAP" .

Parametro	Descrizione	Esempio
`smbShare`	È possibile specificare uno dei seguenti elementi: il nome di una condivisione SMB creata tramite Microsoft Management Console o ONTAP CLI; un nome per consentire a Trident di creare la condivisione SMB; oppure è possibile lasciare il parametro vuoto per impedire l'accesso comune alla condivisione ai volumi. Questo parametro è facoltativo per ONTAP on-premise. Questo parametro è obbligatorio per i backend Amazon FSx per ONTAP e non può essere vuoto.	`smb-share`
`nasType`	**Deve essere impostato su `smb` .** Se nullo, il valore predefinito è `nfs` .	`smb`
`securityStyle`	Stile di sicurezza per i nuovi volumi. **Deve essere impostato su `ntfs` O `mixed` per volumi SMB.**	`ntfs`O `mixed` per volumi SMB
`unixPermissions`	Modalità per nuovi volumi. **Deve essere lasciato vuoto per i volumi SMB.**	""

Abilita SMB sicuro

A partire dalla versione 25.06, NetApp Trident supporta il provisioning sicuro dei volumi SMB creati utilizzando `ontap-nas` E `ontap-nas-economy` backend. Quando è abilitato SMB sicuro, è possibile fornire un accesso controllato alle condivisioni SMB per gli utenti e i gruppi di utenti di Active Directory (AD) utilizzando gli elenchi di controllo di accesso (ACL).

Punti da ricordare

- Importazione `ontap-nas-economy` volumi non è supportato.
- Sono supportati solo i cloni di sola lettura per `ontap-nas-economy` volumi.
- Se Secure SMB è abilitato, Trident ignorerà la condivisione SMB menzionata nel backend.
- L'aggiornamento dell'annotazione PVC, dell'annotazione della classe di archiviazione e del campo backend non aggiorna l'ACL della condivisione SMB.
- L'ACL di condivisione SMB specificato nell'annotazione del PVC clone avrà la precedenza su quelli presenti nel PVC di origine.
- Assicurati di fornire utenti AD validi quando abiliti SMB sicuro. Gli utenti non validi non verranno aggiunti all'ACL.
- Se si forniscono autorizzazioni diverse allo stesso utente AD nel backend, nella classe di archiviazione e nel PVC, la priorità delle autorizzazioni sarà: PVC, classe di archiviazione e quindi backend.
- Secure SMB è supportato per `ontap-nas` importazioni di volumi gestiti e non applicabile alle importazioni di volumi non gestiti.

Passi

1. Specificare adAdminUser in TridentBackendConfig come mostrato nell'esempio seguente:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.193.176.x
  svm: svm0
  useREST: true
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

2. Aggiungere l'annotazione nella classe di archiviazione.

   Aggiungi il `trident.netapp.io/smbShareAdUser` annotazione alla classe di archiviazione per abilitare SMB sicuro senza errori. Il valore utente specificato per l'annotazione `trident.netapp.io/smbShareAdUser` dovrebbe essere lo stesso del nome utente specificato nel `smbcreds` segreto. Puoi scegliere una delle seguenti opzioni per `smbShareAdUserPermission` : `full_control` , `change` , O `read` . L'autorizzazione predefinita è `full_control` .

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

1. Creare un PVC.

   L'esempio seguente crea un PVC:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/snapshotDirectory: "true"
    trident.netapp.io/smbShareAccessControl: |
      read:
        - tridentADtest
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

Opzioni ed esempi di configurazione del NAS ONTAP

Scopri come creare e utilizzare i driver ONTAP NAS con l'installazione Trident . Questa sezione fornisce esempi di configurazione del backend e dettagli per il mapping dei backend alle StorageClass.

Opzioni di configurazione del backend

Per le opzioni di configurazione del backend, consultare la seguente tabella:

Parametro	Descrizione	Predefinito
`version`		Sempre 1
`storageDriverName`	Nome del driver di archiviazione	`ontap-nas`, `ontap-nas-economy` , O `ontap-nas-flexgroup`
`backendName`	Nome personalizzato o backend di archiviazione	Nome del driver + "_" + dataLIF
`managementLIF`	Indirizzo IP di un cluster o di un LIF di gestione SVM. È possibile specificare un nome di dominio completo (FQDN). Può essere impostato per utilizzare indirizzi IPv6 se Trident è stato installato utilizzando il flag IPv6. Gli indirizzi IPv6 devono essere definiti tra parentesi quadre, ad esempio `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` . Per un passaggio senza interruzioni a MetroCluster , vedereEsempio MetroCluster .	"10.0.0.1", "[2001:1234:abcd::fefe]"

Parametro	Descrizione	Predefinito
`dataLIF`	Indirizzo IP del protocollo LIF. NetApp consiglia di specificare `dataLIF` . Se non specificato, Trident recupera i dataLIF dall'SVM. È possibile specificare un nome di dominio completo (FQDN) da utilizzare per le operazioni di montaggio NFS, consentendo di creare un DNS round-robin per bilanciare il carico su più dataLIF. Può essere modificato dopo l'impostazione iniziale. Fare riferimento a . Può essere impostato per utilizzare indirizzi IPv6 se Trident è stato installato utilizzando il flag IPv6. Gli indirizzi IPv6 devono essere definiti tra parentesi quadre, ad esempio `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` . **Omettere per Metrocluster.** Vedi ilEsempio MetroCluster .	Indirizzo specificato o derivato da SVM, se non specificato (non consigliato)
`svm`	Macchina virtuale di archiviazione da utilizzare **Ometti per Metrocluster.** Vedi ilEsempio MetroCluster .	Derivato se un SVM `managementLIF` è specificato
`autoExportPolicy`	Abilita la creazione e l'aggiornamento automatici dei criteri di esportazione [Booleano]. Utilizzando il `autoExportPolicy` E `autoExportCIDRs` opzioni, Trident può gestire automaticamente le policy di esportazione.	falso
`autoExportCIDRs`	Elenco di CIDR per filtrare gli IP dei nodi di Kubernetes quando `autoExportPolicy` è abilitato. Utilizzando il `autoExportPolicy` E `autoExportCIDRs` opzioni, Trident può gestire automaticamente le policy di esportazione.	["0.0.0.0/0", "::/0"]`
`labels`	Insieme di etichette arbitrarie formattate in JSON da applicare ai volumi	""
`clientCertificate`	Valore codificato in Base64 del certificato client. Utilizzato per l'autenticazione basata su certificato	""
`clientPrivateKey`	Valore codificato in Base64 della chiave privata del client. Utilizzato per l'autenticazione basata su certificato	""
`trustedCACertificate`	Valore codificato in Base64 del certificato CA attendibile. Opzionale. Utilizzato per l'autenticazione basata su certificato	""
`username`	Nome utente per connettersi al cluster/SVM. Utilizzato per l'autenticazione basata sulle credenziali. Per l'autenticazione di Active Directory, vedere "Autenticare Trident su un SVM backend utilizzando le credenziali di Active Directory".	
`password`	Password per connettersi al cluster/SVM. Utilizzato per l'autenticazione basata sulle credenziali. Per l'autenticazione di Active Directory, vedere "Autenticare Trident su un SVM backend utilizzando le credenziali di Active Directory".	

Parametro	Descrizione	Predefinito
`storagePrefix`	Prefisso utilizzato durante il provisioning di nuovi volumi nell'SVM. Non può essere aggiornato dopo averlo impostato Quando si utilizza ontap-nas-economy e un prefisso storage di 24 o più caratteri, i qtree non avranno il prefisso storage incorporato, sebbene sarà presente nel nome del volume.	"tridente"
`aggregate`	Aggregato per il provisioning (facoltativo; se impostato, deve essere assegnato all'SVM). Per il `ontap-nas-flexgroup` driver, questa opzione viene ignorata. Se non assegnato, è possibile utilizzare uno qualsiasi degli aggregati disponibili per eseguire il provisioning di un volume FlexGroup . Quando l'aggregato viene aggiornato in SVM, viene aggiornato automaticamente in Trident interrogando SVM senza dover riavviare Trident Controller. Dopo aver configurato un aggregato specifico in Trident per il provisioning dei volumi, se l'aggregato viene rinominato o spostato fuori dall'SVM, il backend passerà allo stato di errore in Trident durante l'interrogazione dell'aggregato SVM. Per riportare online il backend, è necessario modificare l'aggregato con uno presente sull'SVM oppure rimuoverlo del tutto.	""
`limitAggregateUsage`	Il provisioning non riesce se l'utilizzo è superiore a questa percentuale. **Non si applica ad Amazon FSx per ONTAP**.	"" (non applicato di default)

Parametro	Descrizione	Predefinito
flexgroupAggregateList	Elenco degli aggregati per il provisioning (facoltativo; se impostato, deve essere assegnato all'SVM). Tutti gli aggregati assegnati all'SVM vengono utilizzati per effettuare il provisioning di un volume FlexGroup . Supportato per il driver di archiviazione **ontap-nas-flexgroup**. Quando l'elenco aggregato viene aggiornato in SVM, l'elenco viene aggiornato automaticamente in Trident interrogando SVM senza dover riavviare Trident Controller. Dopo aver configurato un elenco di aggregati specifico in Trident per il provisioning dei volumi, se l'elenco di aggregati viene rinominato o spostato fuori da SVM, il backend passerà allo stato di errore in Trident durante l'interrogazione dell'aggregato SVM. Per riportare online il backend, è necessario modificare l'elenco aggregato con uno presente sull'SVM oppure rimuoverlo del tutto.	""
`limitVolumeSize`	Il provisioning non riesce se la dimensione del volume richiesto è superiore a questo valore. Limita inoltre la dimensione massima dei volumi che gestisce per i qtree e `qtreesPerFlexvol` l'opzione consente di personalizzare il numero massimo di qtree per FlexVol volume	"" (non applicato di default)
`debugTraceFlags`	Flag di debug da utilizzare durante la risoluzione dei problemi. Esempio, {"api":false, "method":true} Non utilizzare `debugTraceFlags` a meno che non si stia risolvendo un problema e si necessiti di un dump di registro dettagliato.	null
`nasType`	Configurare la creazione di volumi NFS o SMB. Le opzioni sono `nfs` , `smb` o nullo. Impostando il valore su null, i volumi NFS vengono impostati di default.	`nfs`
`nfsMountOptions`	Elenco separato da virgole delle opzioni di montaggio NFS. Le opzioni di montaggio per i volumi persistenti di Kubernetes sono normalmente specificate nelle classi di archiviazione, ma se non vengono specificate opzioni di montaggio in una classe di archiviazione, Trident utilizzerà le opzioni di montaggio specificate nel file di configurazione del backend di archiviazione. Se non vengono specificate opzioni di montaggio nella classe di archiviazione o nel file di configurazione, Trident non imposterà alcuna opzione di montaggio su un volume persistente associato.	""

Parametro	Descrizione	Predefinito
`qtreesPerFlexvol`	Il numero massimo di Qtree per FlexVol deve essere compreso nell'intervallo [50, 300]	"200"
`smbShare`	È possibile specificare uno dei seguenti elementi: il nome di una condivisione SMB creata tramite Microsoft Management Console o ONTAP CLI; un nome per consentire a Trident di creare la condivisione SMB; oppure è possibile lasciare il parametro vuoto per impedire l'accesso comune alla condivisione ai volumi. Questo parametro è facoltativo per ONTAP on-premise. Questo parametro è obbligatorio per i backend Amazon FSx per ONTAP e non può essere vuoto.	`smb-share`
`useREST`	Parametro booleano per utilizzare le API REST ONTAP . `useREST`Quando impostato su `true` , Trident utilizza le API REST ONTAP per comunicare con il backend; quando impostato su `false` Trident utilizza chiamate ONTAPI (ZAPI) per comunicare con il backend. Questa funzionalità richiede ONTAP 9.11.1 e versioni successive. Inoltre, il ruolo di accesso ONTAP utilizzato deve avere accesso a `ontapi` applicazione. Ciò è soddisfatto dal predefinito `vsadmin` E `cluster-admin` ruoli. A partire dalla versione Trident 24.06 e ONTAP 9.15.1 o successiva, `useREST` è impostato su `true` per impostazione predefinita; modifica `useREST` A `false` per utilizzare le chiamate ONTAPI (ZAPI).	`true`per ONTAP 9.15.1 o successivo, altrimenti `false` .
`limitVolumePoolSize`	Dimensione massima FlexVol richiedibile quando si utilizzano Qtrees nel backend ontap-nas-economy.	"" (non applicato di default)
`denyNewVolumePools`	Limita `ontap-nas-economy` backend dalla creazione di nuovi volumi FlexVol per contenere i loro Qtree. Per il provisioning di nuovi PV vengono utilizzati solo i Flexvol preesistenti.	
`adAdminUser`	Utente o gruppo di utenti amministratore di Active Directory con accesso completo alle condivisioni SMB. Utilizzare questo parametro per fornire diritti di amministratore alla condivisione SMB con controllo completo.	

Opzioni di configurazione del backend per il provisioning dei volumi

È possibile controllare il provisioning predefinito utilizzando queste opzioni in `defaults` sezione della configurazione. Per un esempio, vedere gli esempi di configurazione riportati di seguito.

Parametro	Descrizione	Predefinito
`spaceAllocation`	Assegnazione dello spazio per Qtrees	"VERO"

Parametro	Descrizione	Predefinito
`spaceReserve`	Modalità di prenotazione dello spazio; "nessuno" (sottile) o "volume" (spesso)	"nessuno"
`snapshotPolicy`	Criterio di snapshot da utilizzare	"nessuno"
`qosPolicy`	Gruppo di criteri QoS da assegnare ai volumi creati. Scegli uno tra qosPolicy o adaptiveQosPolicy per pool di archiviazione/backend	""
`adaptiveQosPolicy`	Gruppo di policy QoS adattivo da assegnare ai volumi creati. Scegliere tra qosPolicy o adaptiveQosPolicy per ogni pool di archiviazione/backend. Non supportato da ontap-nas-economy.	""
`snapshotReserve`	Percentuale di volume riservata agli snapshot	"0" se `snapshotPolicy` è "nessuno", altrimenti ""
`splitOnClone`	Dividere un clone dal suo genitore al momento della creazione	"falso"
`encryption`	Abilita NetApp Volume Encryption (NVE) sul nuovo volume; l'impostazione predefinita è `false` . Per utilizzare questa opzione, NVE deve essere concesso in licenza e abilitato sul cluster. Se NAE è abilitato sul backend, qualsiasi volume fornito in Trident sarà abilitato per NAE. Per maggiori informazioni, fare riferimento a:"Come funziona Trident con NVE e NAE" .	"falso"
`tieringPolicy`	Criterio di tiering per utilizzare "nessuno"	
`unixPermissions`	Modalità per nuovi volumi	"777" per i volumi NFS; vuoto (non applicabile) per i volumi SMB
`snapshotDir`	Controlla l'accesso al `.snapshot` elenco	"true" per NFSv4 "false" per NFSv3
`exportPolicy`	Politica di esportazione da utilizzare	"predefinito"
`securityStyle`	Stile di sicurezza per i nuovi volumi. Supporti NFS `mixed` E `unix` stili di sicurezza. Supporti SMB `mixed` E `ntfs` stili di sicurezza.	L'impostazione predefinita di NFS è `unix` . L'impostazione predefinita di SMB è `ntfs` .
`nameTemplate`	Modello per creare nomi di volume personalizzati.	""

Per utilizzare i gruppi di policy QoS con Trident è necessario ONTAP 9.8 o versione successiva. Dovresti utilizzare un gruppo di policy QoS non condiviso e assicurarti che il gruppo di policy venga applicato individualmente a ciascun componente. Un gruppo di policy QoS condiviso impone il limite massimo per la produttività totale di tutti i carichi di lavoro.

Esempi di provisioning del volume

Ecco un esempio con i valori predefiniti definiti:

```
---
version: 1
storageDriverName: ontap-nas
backendName: customBackendName
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
labels:
  k8scluster: dev1
  backend: dev1-nasbackend
svm: trident_svm
username: cluster-admin
password: <password>
limitAggregateUsage: 80%
limitVolumeSize: 50Gi
nfsMountOptions: nfsvers=4
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: premium
  exportPolicy: myk8scluster
  snapshotPolicy: default
  snapshotReserve: "10"
```

Per `ontap-nas` E `ontap-nas-flexgroups` , Trident ora utilizza un nuovo calcolo per garantire che FlexVol sia dimensionato correttamente con la percentuale snapshotReserve e PVC. Quando l'utente richiede un PVC, Trident crea il FlexVol originale con più spazio utilizzando il nuovo calcolo. Questo calcolo garantisce che l'utente riceva lo spazio scrivibile richiesto nel PVC e non uno spazio inferiore a quello richiesto. Prima della versione 21.07, quando l'utente richiedeva un PVC (ad esempio, 5 GiB), con snapshotReserve al 50%, otteneva solo 2,5 GiB di spazio scrivibile. Questo perché ciò che l'utente ha richiesto è l'intero volume e `snapshotReserve` è una percentuale di quello. Con Trident 21.07, ciò che l'utente richiede è lo spazio scrivibile e Trident definisce lo `snapshotReserve` numero come percentuale del volume totale. Questo non si applica a `ontap-nas-economy` . Per vedere come funziona, vedere l'esempio seguente

Il calcolo è il seguente:

```
Total volume size = (PVC requested size) / (1 - (snapshotReserve
percentage) / 100)
```

Per snapshotReserve = 50% e richiesta PVC = 5 GiB, la dimensione totale del volume è 5/.5 = 10 GiB e la dimensione disponibile è 5 GiB, che è ciò che l'utente ha richiesto nella richiesta PVC IL `volume show` il comando dovrebbe mostrare risultati simili a questo esempio:

I backend esistenti delle installazioni precedenti eseguiranno il provisioning dei volumi come spiegato sopra durante l'aggiornamento Trident. Per i volumi creati prima dell'aggiornamento, è necessario ridimensionarli affinché la modifica venga visualizzata. Ad esempio, un PVC da 2 GiB con `snapshotReserve=50` in precedenza produceva un volume che forniva 1 GiB di spazio scrivibile. Ridimensionando il volume a 3 GiB, ad esempio, l'applicazione ottiene 3 GiB di spazio scrivibile su un volume da 6 GiB.

Esempi di configurazione minima

Gli esempi seguenti mostrano configurazioni di base che lasciano la maggior parte dei parametri predefiniti. Questo è il modo più semplice per definire un backend.

> Se si utilizza Amazon FSx su NetApp ONTAP con Trident, si consiglia di specificare i nomi DNS per i LIF anziché gli indirizzi IP.

Esempio di economia NAS ONTAP

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

Esempio di ONTAP NAS Flexgroup

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

Esempio MetroCluster

È possibile configurare il backend per evitare di dover aggiornare manualmente la definizione del backend dopo il passaggio e il ritorno durante"Replica e ripristino SVM" .

Per un passaggio e un ritorno senza interruzioni, specificare l'SVM utilizzando `managementLIF` e omettere il `dataLIF` E `svm` parametri. Per esempio:

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 192.168.1.66
username: vsadmin
password: password
```

Esempio di volumi SMB

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
nasType: smb
securityStyle: ntfs
unixPermissions: ""
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

Esempio di autenticazione basata su certificato

Questo è un esempio minimo di configurazione backend. `clientCertificate` , `clientPrivateKey` , E `trustedCACertificate` (facoltativo, se si utilizza una CA attendibile) vengono popolati in `backend.json` e prendere rispettivamente i valori codificati in base64 del certificato client, della chiave privata e del certificato CA attendibile.

```
---
version: 1
backendName: DefaultNASBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.15
svm: nfs_svm
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

Esempio di policy di esportazione automatica

Questo esempio mostra come è possibile istruire Trident a utilizzare criteri di esportazione dinamici per creare e gestire automaticamente i criteri di esportazione. Funziona allo stesso modo per il `ontap-nas-economy` E `ontap-nas-flexgroup` conducenti.

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-nasbackend
autoExportPolicy: true
autoExportCIDRs:
- 10.0.0.0/24
username: admin
password: password
nfsMountOptions: nfsvers=4
```

Esempio di indirizzi IPv6

Questo esempio mostra `managementLIF` utilizzando un indirizzo IPv6.

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas_ipv6_backend
managementLIF: "[5c5d:5edf:8f:7657:bef8:109b:1b41:d491]"
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-ontap-ipv6
svm: nas_ipv6_svm
username: vsadmin
password: password
```

Esempio Amazon FSx per ONTAP che utilizza volumi SMB

IL `smbShare` il parametro è obbligatorio per FSx per ONTAP che utilizza volumi SMB.

```
---
version: 1
backendName: SMBBackend
storageDriverName: ontap-nas
managementLIF: example.mgmt.fqdn.aws.com
nasType: smb
dataLIF: 10.0.0.15
svm: nfs_svm
smbShare: smb-share
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

Esempio di configurazione del backend con nameTemplate

```
---
version: 1
storageDriverName: ontap-nas
backendName: ontap-nas-backend
managementLIF: <ip address>
svm: svm0
username: <admin>
password: <password>
defaults:
  nameTemplate:
"{{.volume.Name}}_{{.labels.cluster}}_{{.volume.Namespace}}_{{.vo\
    lume.RequestName}}"
labels:
  cluster: ClusterA
  PVC: "{{.volume.Namespace}}_{{.volume.RequestName}}"
```

Esempi di backend con pool virtuali

Nei file di definizione backend di esempio mostrati di seguito, vengono impostati valori predefiniti specifici per tutti i pool di archiviazione, ad esempio `spaceReserve` a nessuno, `spaceAllocation` a falso, e `encryption` a falso. I pool virtuali sono definiti nella sezione storage.

Trident imposta le etichette di provisioning nel campo "Commenti". I commenti sono impostati su FlexVol per `ontap-nas` o FlexGroup per `ontap-nas-flexgroup` . Trident copia tutte le etichette presenti su un pool virtuale nel volume di archiviazione al momento del provisioning. Per comodità, gli amministratori di storage possono definire etichette per pool virtuale e raggruppare i volumi in base all'etichetta.

In questi esempi, alcuni dei pool di archiviazione impostano i propri `spaceReserve` , `spaceAllocation` , E `encryption` valori e alcuni pool sovrascrivono i valori predefiniti.

Esempio ONTAP NAS

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
svm: svm_nfs
username: admin
password: <password>
nfsMountOptions: nfsvers=4
defaults:
  spaceReserve: none
  encryption: "false"
  qosPolicy: standard
labels:
  store: nas_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      app: msoffice
      cost: "100"
    zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: "true"
      unixPermissions: "0755"
      adaptiveQosPolicy: adaptive-premium
  - labels:
      app: slack
      cost: "75"
    zone: us_east_1b
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      department: legal
      creditpoints: "5000"
    zone: us_east_1b
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      app: wordpress
```

```
      cost: "50"
    zone: us_east_1c
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0775"
  - labels:
      app: mysqldb
      cost: "25"
    zone: us_east_1d
    defaults:
      spaceReserve: volume
      encryption: "false"
      unixPermissions: "0775"
```

Esempio di ONTAP NAS FlexGroup

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: "false"
labels:
  store: flexgroup_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      protection: gold
      creditpoints: "50000"
    zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      protection: gold
      creditpoints: "30000"
    zone: us_east_1b
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      protection: silver
      creditpoints: "20000"
    zone: us_east_1c
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0775"
  - labels:
      protection: bronze
      creditpoints: "10000"
    zone: us_east_1d
    defaults:
```

```
      spaceReserve: volume
      encryption: "false"
      unixPermissions: "0775"
```

Esempio di economia NAS ONTAP

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: "false"
labels:
  store: nas_economy_store
region: us_east_1
storage:
  - labels:
      department: finance
      creditpoints: "6000"
    zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      protection: bronze
      creditpoints: "5000"
    zone: us_east_1b
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0755"
  - labels:
      department: engineering
      creditpoints: "3000"
    zone: us_east_1c
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0775"
  - labels:
      department: humanresource
      creditpoints: "2000"
    zone: us_east_1d
    defaults:
      spaceReserve: volume
```

```
      encryption: "false"
      unixPermissions: "0775"
```

Mappa i backend su StorageClasses

Le seguenti definizioni StorageClass fanno riferimento a Esempi di backend con pool virtuali . Utilizzando il `parameters.selector` campo, ogni StorageClass richiama quali pool virtuali possono essere utilizzati per ospitare un volume. Il volume avrà gli aspetti definiti nel pool virtuale scelto.

- IL `protection-gold` StorageClass verrà mappato sul primo e sul secondo pool virtuale in `ontap-nas-flexgroup` backend. Queste sono le uniche piscine che offrono una protezione di livello Gold.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=gold"
  fsType: "ext4"
```

- IL `protection-not-gold` StorageClass verrà mappato sul terzo e quarto pool virtuale in `ontap-nas-flexgroup` backend. Questi sono gli unici pool che offrono un livello di protezione diverso dall'oro.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
```

- IL `app-mysqldb` StorageClass verrà mappato sul quarto pool virtuale nel `ontap-nas` backend. Questo è l'unico pool che offre la configurazione del pool di archiviazione per l'app di tipo mysqldb.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: csi.trident.netapp.io
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
```

- Il `protection-silver-creditpoints-20k` StorageClass verrà mappato sul terzo pool virtuale in `ontap-nas-flexgroup` backend. Questo è l'unico pool che offre protezione di livello Silver e 20.000 punti di credito.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"
```

- IL `creditpoints-5k` StorageClass verrà mappato sul terzo pool virtuale in `ontap-nas` backend e il secondo pool virtuale nel `ontap-nas-economy` backend. Queste sono le uniche offerte di pool con 5000 punti di credito.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: csi.trident.netapp.io
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"
```

Trident deciderà quale pool virtuale selezionare e garantirà che i requisiti di archiviazione siano soddisfatti.

Aggiornamento `dataLIF` dopo la configurazione iniziale

È possibile modificare il dataLIF dopo la configurazione iniziale eseguendo il comando seguente per fornire il nuovo file JSON backend con il dataLIF aggiornato.

```
tridentctl update backend <backend-name> -f <path-to-backend-json-file-
with-updated-dataLIF>
```

Se i PVC sono collegati a uno o più pod, è necessario disattivare tutti i pod corrispondenti e quindi riattivarli affinché il nuovo dataLIF abbia effetto.

Esempi di SMB sicuri

Configurazione backend con driver ontap-nas

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Configurazione backend con driver ontap-nas-economy

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas-economy
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Configurazione backend con pool di archiviazione

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm0
  useREST: false
  storage:
  - labels:
      app: msoffice
    defaults:
      adAdminUser: tridentADuser
  nasType: smb
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Esempio di classe di archiviazione con driver ontap-nas

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADtest
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Assicurati di aggiungere `annotations` per abilitare SMB sicuro. Secure SMB non funziona senza annotazioni, indipendentemente dalle configurazioni impostate nel Backend o nel PVC.

Esempio di classe di archiviazione con driver ontap-nas-economy

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser3
parameters:
  backendType: ontap-nas-economy
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Esempio PVC con un singolo utente AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      change:
        - tridentADtest
      read:
        - tridentADuser
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

Esempio PVC con più utenti AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-test-pvc
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      full_control:
        - tridentTestuser
        - tridentuser
        - tridentTestuser1
        - tridentuser1
      change:
        - tridentADuser
        - tridentADuser1
        - tridentADuser4
        - tridentTestuser2
      read:
        - tridentTestuser2
        - tridentTestuser3
        - tridentADuser2
        - tridentADuser3
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
```

Informazioni sul copyright

Informazioni sul marchio commerciale